

# MANAJEMEN JARINGAN KOMPUTER

## (Network computer Management)

Susanto

Fakultas Teknologi Informasi dan Komunikasi Universitas Semarang

### Abstract

*Network computer system the made is not absolute of sure cure to make business more successful, lastt only can be optimal existing system, computer cannot alter bad system become good system. Individual consumer supported by administrator in charge of computer network system perform.ance, representmg component most important in network system, where they earn to exploit as maximum or on the contrary bring to deep ruination.*

Keyword : Network, Computer system

### 1. PENDAHULUAN

Seiring dengan besarnya volume informasi yang ditangani, komputer pribadi dirasakan mulai usang, karena mulai ditemukan hambatan, proses penyebaran dan komunikasi informasi diantara pemakai, masing-masing dengan komputer pribadinya berjalan lambat dan mudah menimbulkan kesalahan. (Stallings, 1985)

Namun karena adanya perkembangan dunia komputer baik perangkat keras maupun perangkat lunak yang sangat pesat, masalah tersebut dapat diselesaikan yaitu dengan menghubungkan komputer pribadi satu dengan komputer pribadi lainnya dalam suatu jaringan komputer lokal maupun dengan jaringan komputer global/dunia.

Melalui tulisan ini akan dibahas mengenai Manajemen jaringan komputer yang bisa dijadikan salah satu pertimbangan di dalam mengelola jaringan agar dapat dimanfaatkan secara benar dan optimal.

Dalam dunia komputer, jaringan berupaya sebaik mungkin dalam memenuhi kebutuhan informasi dan komunikasi pasar bisnis, berkembang dan dapat mempersempit jangkauan pilihan yang ada. Semua juga tergantung pada lingkungan, dan seberapa jauh bisnis dapat mempertahankan keuntungan yang

dihasilkan dalam era kemajuan infonnasi. Upaya menunggu teknologi yang terus berkembang memang ada manfaatnya : harga seniakin turun, teknologi semakin hebat. Tetapi menunggu juga merugikan : bisnis dengan akses teknologi informasi modem selalu memiliki keunggulan kompetitif dibanding saingannya yang terbatas dalam hal teknologi. Beberapa keuntungan jaringan dapat disebutkan disini :

#### 1. Memungkinkan *Resource sharing*.

Pengguna dapat berbagi pakai sumber daya yang terdapat dan terhubung ke jaringan komputer tersebut. Sumber daya tersebut dapat berupa perangkat keras seperti printer dari masing-masing meja kerja, maupun perangkat lunak seperti pembelian lisensi perangkat lunak menjadi lebih murah dibandingkan membeli tiseni *stand-alone* sebanyak sejumlah pengguna.

#### 2. Membantu mempertahankan infonnasi agar tetap ada dan *up-to-date*.

Dengan sistem data terpusat yang dikelola dengan baik memungkinkan banyak pengguna mengakses data dari berbagai lokasi yang berbeda.

#### 3. Membantu mempercepat proses berbagi data ( *data sharing* )

Mentransfer file pada jaringan lebih cepat dibandingkan sarana berbagi file lainnya yang bukan jaringan.

4. Memungkinkan kelompok kerja berkomunikasi dengan lebih efisien.  
Surat elektronik (e-mail) dan penyampaian pesan elektronik merupakan substansi sebagian besar sistem jaringan, disamping pemantauan proyek, konferensi on-line, groupware dimana semua bertujuan membantuk team kerja lebih produktif.
5. Membantu pelaku bisnis dalam melayani klien mereka dengan lebih efektif  
Akses jarak jauh ke data terpusat memudahkan karyawan melayani klien di lapangan, dan klien dapat berkomunikasi langsung dengan pemasok.

### 1.1 Jaringan di Tempat Kerja

Terdapat beberapa fakta sehari-hari yang menunjukkan bahwa penerapan sistem jaringan dapat membantu bisnis Anda berfungsi lebih efisien dari masalah berikut :

- Hilangnya data karena sebagian individu tidak membuat backup disamping sebab-sebab lain
- Semakin besarnya volume file yang ditransfer melalui floppy disk
- Komunikasi bisnis rutin yang dilakukan secara serampangan dengan tujuan tertentu, atau mengatur pertemuan formal untuk membahas masalah sehari-hari
- Pesan penting yang dikirim melalui catatan, atau secarik kertas, hilang atau tidak diperhatikan, atau kadaluwarsa

Namun sistem jaringan komputer yang dibuat bukanlah mutlak obat mujarab untuk membuat bisnis lebih sukses, hanya saja dapat mengoptimalkan sistem yang ada, komputer tidak dapat mengubah sistem yang buruk menjadi sistem yang baik. Pengguna individu didukung oleh administrator yang bertanggung jawab atas kinerja sistem jaringan komputer, merupakan komponen paling penting dalam

sistem jaringan tersebut, dimana mereka dapat memanfaatkan semaksimal mungkin atau sebaliknya membawa ke jurang kehancuran.

Saat beralih dari lingkup stand-alone ke jaringan, pemilihan administrator yang cocok dengan kebutuhan lingkungan bisnis sangat menentukan. Administrator harus orang yang dapat dipercaya dan harus terlibat dalam setiap aspek rancangan, pemilihan, dan implementasi, sistem jaringan. Selain administrator juga dibutuhkan personil lain tergantung kompleks tidaknya jaringan komputer :

- Administrator database  
Bertanggung jawab terhadap pemrograman dan pemeliharaan multirelasi database raksasa dalam lingkup jaringan, dan mengatur kemudahan akses langsung ke database oleh pengguna jaringan.
- Manager kelompok kerja  
Bertanggung jawab atas pemecahan masalah, implementasi standar dan solusi, peninjauan kinerja, peningkatan efisiensi kelompok individu tertentu yang terhubung sebagai suatu kelompok, ke lingkup jaringan yang lebih besar.
- Staff Pendukung  
Bertanggung jawab memberi bantuan teknis kepada administrator sistem dalam lingkup jaringan yang besar dan kompleks. Memberikan solusi pemecahan masalah rutin serta pelatihan di tempat pengguna.
- Kontraktor pemeliharaan  
Bertanggung jawab atas perbaikan dan upgrade perangkat keras, biasanya dengan melakukan perjanjian dengan pihak ketiga atau penjual.

Namun, Apabila jaringan komputer cukup besar, maka tanggung jawab manajemen dapat dibagi-bagi di antara anggota team manajemen tetap, terlepas apakah kewajiban ini dipikul oleh satu orang atau team, keberhasilan jaringan komputer sangat ditentukan oleh siapa yang mengelolanya.

Manager jaringan yang baik memikul tanggung jawab mendasar berikut berkenaan dengan jaringan. Mereka harus :

- Memahami sistem
- Memelihara backup
- Memelihara keamanan
- Memelihara sistem log
- Mengelola percetakan
- Memantau seluruh fungsi jaringan agar didapat efisiensi maksimum
- Mengevaluasi dan memelihara aplikasi
- Mengikuti perubahan dan pembaruan yang terjadi dalam dunia industri.

## 2. MEMAHAMI SISTEM

Untuk memahami sistem anda, manager yang baik memerlukan dua hal : pengetahuan tentang ciri teknis (yang didapat dari pelatihan formal), serta pengetahuan tentang kinerja nyata, yang hanya dapat diperoleh dari pengalaman sehari-hari. Dengan perkataan lain semakin lama manager tersebut bekerja dengan sistem Anda, semakin baik kualitasnya.

Berkenaan dengan jenis aplikasi yang terkait khusus dengan jaringan, manager mungkin merasa lebih efisien apabila aplikasi disimpan pada server, bahkan mungkin harus demikian. Hal ini dapat terjadi untuk aplikasi seperti perangkat lunak server database SQL, yang bekerja langsung dengan database yang digunakan bersama pada server dan mengirim hasil pemrosesannya ke *workstation*. Apabila jenis perangkat lunak ini dijalankan secara lokal, maka hampir tidak ada peningkatan kinerja yang didapat. Namun, database *front-end* (aplikasi yang memformat hasil query SQL) belum tentu dapat dijalankan dengan efisien dari hard disk lokal; manager mungkin harus menguji konfigurasi yang berbeda untuk mengetahui sampai seberapa baik jika dijalankan pada sistem Anda.

## 3. MEMELIHARA BACKUP

Media penyimpanan tape sangat berguna sebagai media backup karena cartridge dapat dibawa ke tempat terpisah yang aman, seperti kotak deposit bank yang aman. Sistem backup tape juga memiliki kelemahan; sistem ini agak kaku apabila Anda ingin memulihkan satu atau dua file saja.

### a. Apa Yang Harus Di Backup

Anda perlu membackup membaca file data lebih sering dibandingkan file perangkat lunak aplikasi. Apabila Anda memiliki disk instalasi asli, buatlah backupnya sebelum perangkat lunak ini di instal. Apabila Anda menginstal dari perangkat lunak dari disk CD-ROM, atau apabila proses instalasi dan konfigurasi cukup kompleks, Anda mungkin perlu membuat backup dari file yang di instal di luar hard disk, agar tidak perlu menginstal ulang aplikasi dari awal.

Backup file konfigurasi untuk perangkat aplikasi secara terpisah. Buat backup baru file konfigurasi setiap kali Anda memperbarui konfigurasi karena alasan tertentu.

Apabila struktur direktori terorganisasi dengan baik, Anda harus menyimpan file data dalam direktori yang terpisah dari file aplikasi perangkat lunak. Perangkat lunak backup otomatis memungkinkan Anda menetapkan secara tepat direktori mana (dan file nama dalam direktori tersebut) yang perlu di backup secara teratur.

Disamping file data sehari-hari, Anda juga harus membuat backup teratur untuk data sistem jaringan Anda. Jaringan yang berbeda mengelola data sistemnya dengan cara yang berbeda pula, tetapi beberapa contoh jenis file sistem yang perlu Anda backup meliputi :

- File keamanan
- Struktur direktori
- File *login scrip*
- File informasi pengguna
- File informasi kelompok kerja file konfigurasi *workstation*

### b. Menentukan siapa yang bertugas melakukan backup system

Beberapa administrator jaringan menyerahkan proses back up kepada user masing-masing. Hal ini berarti setiap user pada sistem bertanggung jawab atas keselamatan file-filenya sendiri. Secara praktis hal ini bukan cara yang baik. Dalam kenyataannya user tidak akan meluangkan waktunya untuk melakukan back up file-filenya secara memadai. Beberapa penelitian menunjukkan bahwa, jika back up file diserahkan kepada user, maka tidak lebih dari 10 persen yang melakukan tugas tersebut secara tetap.

Jadi banyak administrator jaringan memilih untuk melakukan semua tugas back up sebagai bagian dari pemeliharaan rutin mereka terhadap sistem. Administrator jaringan bertanggung-jawab untuk menjaga agar sistem tetap bekerja, memelihara file-file program, dan membentuk fungsi-fungsi pemeliharaan terhadap tugas-tugas tersebut. Juga dalam kenyataannya, administrator jaringan dapat melakukan tugas-tugas back up lebih efisien daripada user yang sangat jarang melakukan tugas tersebut dan seringkali tanpa keahlian yang sama dengan administrator jaringan.

### c. Kapan Harus Membackup

Kebanyakan manager berpengalaman menggunakan bentuk sistem backup yang dikhususkan. Misalnya, mereka mungkin membuat sejumlah tape backup yang baru setiap hari dengan menggunakan kembali tape backup lama setelah kurun waktu tertentu (biasanya satu minggu hingga satu bulan). Metoda ini didasarkan atas pandangan bahwa data backup tersebut akan usang setelah mencapai umur tertentu, sehingga dapat ditindih oleh data yang lebih baru. Penggunaan seri *tape backup* juga memberikan tingkat jaminan tambahan: Seandainya terjadi error pada backup paling baru, Anda dapat berpaling pada backup sebelum itu, sehingga kehilangan juga sedikit sekali.

Disamping membuat backup harian, sebagian manager membuat backup. Lengkap pada interval yang teratur (mungkin sekali seminggu atau sekali atau dua kali dalam sebulan)

### d. Jenis Backup

Terdapat tiga strategi dasar untuk memelihara sejumlah backup :

1. **Full Backup (Backup Lengkap):** Pada full backup, seluruh data penting dibackup. Seperti dapat Anda duga, kerugiannya adalah sangat memakan waktu dan memerlukan ruang simpan backup yang sangat besar. keuntungannya sangat terasa, apabila Anda perlu memulihkan data. Seluruh file data versi paling baru disimpan bersama dalam satu paket besar. Minimal Anda harus membuat full backup setidaknya pada waktu pertama kali Anda mem-backup data Anda.
2. **Incremental Backup (Backup Bertahap) :** Setiap backup ini membaca atribut file guna menentukan file mana yang telah di tambah atau dimodifikasi sejak abackup terakhir. Hanya file yang teala dimodifikasi yang benara-benar di backup. Proses backup ini adalah yang tercepat, karena jumlah file yang disalin juga paling sedikit, namun pekerjaan pemulihan dapat menjadi sesuatu yang sangat membosankan naun terapksa harus dilakukan. Untuk menormalkan kembali sistem yang mengalami kegagalan, Anda harus memulihkan full backup yang pahng baru, diikuti oleh setiap incremental backup yang dilakukan setelah full backup Apabila Anda belum membuat full backup, maka pemulihan yang harus Anda lakukan dapat menjadi pekerjaan yang sangat menjemukan.
3. **Differential Backup (Backup Diferensial) :** Sistem ini, terletak diantara dua jenis backup



terdahulu. Sistem backup ini membaca atribut tanggal file data, dan hanya mem-backup file yang telah di tambah atau diubah setelah full backup terakhir. Seringkali sedikit lebih lama dibandingkan incremental backup, tetapi pemulihannya lebih dapat diprediksikan. Untuk menormalkan kembali sistem yang telah mengalami kegagalan, Anda harus memulihkan full backup terakhir diikuti oleh incremental backup terakhir.

#### e. Perbandingan Backup dan Arsip

Kebanyakan jaringan membutuhkan dua tipe proteksi yang berbeda, yaitu membuat salinan dengan back up dan arsip. Perbedaan dasar antara membuat salinan dengan back up dan membuat salinannya dengan arsip adalah tujuannya. Umumnya back up sistem bertujuan untuk melindungi jaringan dari kesalahan mekanis dan manusia. Salinan dengan back up melindungi jaringan terhadap masalah hardware, misalnya kerusakan hard disk jaringan. Back up ini juga dapat membantu ketika user dengan tidak sengaja menghapus file-file atau program-program.

Tetapi file arsip biasanya dibuat untuk memelihara file-file tertentu dalam jangka waktu tertentu. Misalnya, ingin membuat arsip dari sparesheet atau laporan status setiap bulan. User mungkin ingin membuat file arsip dengan cara yang sama dengan membuat arsip lembaran salinan dari dokumen dalam jangka waktu tertentu.

Prosedur pengarsipan yang baik juga membantu untuk mengelola ruang disk. File-file tertentu tidak perlu tetap disimpan untuk jangka waktu yang lama. Contohnya, file korespondensi umumnya tidak perlu disimpan terus menerus. Karena file-file ini tentu tidak ingin dihapus seluruhnya, maka sebaiknya ada prosedur yang menyimpan file-file ini di suatu tempat.

Seringkali alat yang sama digunakan untuk melakukan kedua tugas tersebut. Kebanyakan utilitas yang ditujukan untuk melakukan back up

file dapat digunakan juga untuk melakukan pengarsipan file tersebut.

#### f. Melakukan Pengarsipan Bulanan File-File

Umumnya pengarsipan perlu dilakukan hanya satu kali dalam sebulan. File-file arsip harus disimpan dalam media berbeda (tape, disk, atau beberapa disk) dari salinan back up. Tujuan pengarsipan adalah berbeda dengan back up file, sehingga prosedur pelaksanaannya pun berbeda. Urutan berikut ini adalah sebuah contoh urutan prosedur pelaksanaan pengarsipan file :

- Tentukan semua direktori dan file yang akan di-arsip
- Tentukan apakah file-file akan tetap disimpan dalam server setelah dilakukan pengarsipan
- Laksanakan proses pengarsipan
- Hapus file-file yang di-arsip dan sudah tidak diperlukan lagi pada server
- Cetak daftar file-file yang di-arsip
- Simpan media yang berisi file-file arsip tersebut di tempat yang aman.

Teknik lain yang banyak dilakukan oleh administrator jaringan ialah file-file yang akan diarsip, di-compress terlebih dahulu. Beberapa utilitas yang baik menyediakan fasilitas compress file ini dan mengumpulkannya ke dalam satu file. Cara compress ini mengurangi jumlah ruang disk yang diperlukan untuk pengarsipan. File-file seringkali dapat dicompress menjadi 50 sampai 80 persen. Jika pengarsipan membutuhkan ruang yang lebih kecil, maka ruang disk pengarsipan dapat menampung lebih banyak, dan berarti mengurangi biaya pengarsipan.

#### 4. MEMELIHARA SYSTEM LOG

Berikut adalah beberapa unsur mendasar dari system log:

- a. **Spesifikasi Perangkat Keras** : Simpan daftar aplikasi seluruh perangkat keras server dan workstation Anda. Daftar ini harus mencakup nama buatan serta model, nomor seri, nomor jaringan internal, informasi garansi, disamping nama pabrik, penjual dan pihak yang menginstal. Sertakan piranti perangkak keras seperti disk drive, network interface card, monitor, printer dan peranti periferil seperti modem. Jangan lupa menyimpan informasi tentang peralatan tambahan {*add-on*) seperti *router* dan *transceiver*. Terakhir, jangan lupa menyimpan catatan pembelian dan kwitansi pembayaran.
- b. **File Boot** : Simpan hasil cetak file boot seluruh server dan workstation Anda; misalnya AUTOEXEC.BAT dan CONFIG.SYS.
- c. **Struktur Direktori** : Simpan hasil-cetak terbaru dari struktur direktori. Tambahkan hasil cetak baru setiap kali Anda memperbarui struktur. Sertakan nama volume dan direktori, atribut dan hak akses. Kebanyakan sistem operasi Jaringan mencakup utility untuk menghasilkan hasil-cetak yang memperlihatkan organisasi direktori serta penyangannya; misalnya, NetWare menggunakan perintah *showname* LISTDIP, untuk menghasilkan cetak tersebut.
- d. **Profil Pengguna** : Minimal simpan hasil-cetak nama mesin tiap pengguna, namanya, kelompoknya, login script dan hak akses.
- e. **Login Script Sistem** : Apabila jaringan Anda menggunakan login script sistem, simpan salinan file berikut catatan tanggalnya. Simpan salinan login script default kalau-kalau pengguna tanpa script individu membutuhkannya.
- f. **Catatan Harian Konfigurasi** : catatan ini memuat riwayat perubahan konfigurasi server dan workstation. Jangan lupa menyertakan catatan konfigurasi perangkat keras yang di install seperti *network interface card*. Sewaktu Anda memperbaharui konfigurasi, simpan hasil cetak versi baru bersama versi lama beserta catatan tanggalnya. Langkah ini sangat membantu dalam menyimpan salinan konfigurasi terdahulu; suatu hari Anda mungkin memerlukan untuk kembali ke konfigurasi lama.
- g. **Catatan Harian Perangkat Lunak** : Catat nomor versi, informasi lisensi dan lokasi aplikasi perangkat lunak yang telah di instal. Catat nama pengguna absah dan siapa yang pada awalnya menginstal perangkat lunak. Seperti yang Anda perbuat terhadap perangkat keras, simpan juga catatan pembelian, garansi dan pembayaran.
- h. **Standar Perangkat Keras dan Perangkat Lunak** : Simpan (dan sebarkan) daftar jenis perangkat keras dan aplikasi perangkat lunak standar yang telah Anda setuju untuk digunakan pada jaringan Anda. Hal ini sama saja dengan menyatakan kebijakan berkenaan dengan jenis perangkat keras dan perangkat lunak yang akan Anda dukung. Pengguna senang sekali menambahkan hal-hal yang sifatnya pribadi pada *workstation* mereka (misalnya *screen saver*), dan kadang item ini mengganggu Jaringan. Apabila Anda memiliki kebijakan dalam hal pemberian dukungan berarti Anda dalam posisi yang menguntungkan dalam menerapkan kontrol serta kepatuhan berkenaan dengan apa yang dapat ditolerir oleh jaringan.

- J. **Jadwal Backup** : Catat pelaksanaan backup data dan file apa saja yang di backup. Apabila Anda menggunakan sistem backup otomatis, maka perangkat lunak backup Anda mungkin mencetak catatan file yang telah di backup, sewaktu backup berlangsung dan apabila terjadi *error* selama proses berlangsung. Apabila Anda mem-backup secara manual, simpan *checklist* (daftar-periksa) yang memperlihatkan bilamana Anda melakukan backup dan jenis backup apa yang diterapkan (*full incremental* atau *differential*).
- j. **Konfigurasi Pencetakan** : Catat konfigurasi printer, nama printer, nomor jaringan internal, port dan interrupt yang digunakan, dan informasi antrian cetak. Karena pencetakan seringkali menimbulkan masalah pada jaringan, maka dokumentasi yang lengkap berkenaan dengan printer dapat membantu banyak.
- k. **Prosedur Keamanan** : Simpan (dan sebarkan) kebijakan tertulis berkenaan dengan prosedur dan hak akses bagi pengguna baru dan pengguna yang ada saat ini. Sertakan hal-hal seperti bilamana password harus diganti, serta batasan jenis password yang telah Anda konfigurasi pada sistem untuk diterima.
5. **MENGEVALUASI APLIKASI**  
Berikut adalah beberapa hal yang perlu dicermati sewaktu mengevaluasi aplikasi guna mengetahui apakah aplikasi bersangkutan memungkinkan untuk diinstalasi pada jaringan Anda:
- a. **Kompatibilitas** : Sebagian besar penjual perangkat lunak pasti akan mengatakan bahwa aplikasi mereka kompatibel dengan jaringan Anda. Tetapi ucapan itu sebaiknya jangan dipegang sebagai sesuatu yang pasti. Sebagian jaringan memiliki ciri yang mungkin akan menimbulkan konflik dengan aplikasi perangkat lunak. Dapatkan garansi dari penjual bahwa, seandainya aplikasi terbukti tidak kompatibel dengan jaringan Anda, Anda dapat mengembalikannya dalam kurun yang wajar dan berasaskan dengan penggantian biaya penuh.
- b. **Dukungan Bagi Banyak Pengguna yang Mengakses Secara Serentak** : Berhati-hatilah sewaktu menginstal aplikasi yang dirancang untuk lingkup *stand-alone*. Meskipun biasanya aplikasi tersebut dapat dijalankan apada jaringan, namun Anda harus berhati-hati dalam mengkonfigurasi jaringan agar hanya satu pengguna yang diijinkan pada saat yang bersamaan untuk mengoperasikan program ini.
- Misalnya, Anda mungkin harus menginstal aplikasi subdirektori pengguna tunggal atau menjalankan aplikasi dengan *script* atau *file batch* khusus yang mengubah hak akses pengguna lain ke file data sementara aplikasi sedang digunakan dan memulihkan hak akses semula sewaktu pengguna keluar dari aplikasi. Masalah konfigurasi ini cukup rumit dan sulit dalam setup dan pemeliharannya.
  - Disamping itu, sewaktu Anda menginstal perangkat lunak stand-alone pada jaringan, Anda mungkin diminta untuk melakukan tindakan tertentu berkenaan dengan biaya lisensi untuk masing-masing pengguna aplikasi.
  - Sedapat mungkin hindari instalasi aplikasi *stand-alone* pada jaringan Anda. Sungguh beruntung, sebagian besar program perangkat lunak terkenal menyediakan versi untuk jaringan.

## 6. KEAMANAN

Terdapat dua aspek keamanan komputer: pertama, memberikan kepada pengguna tertentu ijin untuk mengakses jaringan pada tingkat sembarang; kedua, setelah memberikan akses kepada pengguna yang berhak, memberikan ijin untuk mengakses data tertentu secara terbatas. Keamanan tingkat pertama dilakukan dengan memrogram jaringan agar dapat mengidentifikasi pengguna yang berhak dan menguncinya dari pengguna yang tidak dikenalnya.

### a. Keamanan Akses Jaringan Global

Terdapat tiga cara di mana jaringan Anda dapat mengidentifikasi pengguna dan memberikan kepada mereka ijin untuk mengaksesnya :

- 1) Ijin didasarkan atas Siapa mereka : Sistem ini adalah yang paling aman, karena sistem mengidentifikasi pengguna berdasarkan atribut fisik yang unik sifatnya. Contoh sistem siapa-anda mencakup alat pembaca cetakan jari dan telapak tangan di antara berbagai peranti identifikasi mahal dan canggih lainnya.
- 2) Ijin didasarkan atas apa yang Anda miliki : Sistem ini paling sering digunakan. Sistem mengenali pengguna yang berhak dan memberikan kepada mereka akses apabila mereka memiliki kunci yang harus disisipkan ke dalam alat pengunci atau kartu magnetik yang harus digeserkan melalui alat pembaca kartu (*card reader*). Kelemahan peranti ini terletak pada mudahnya peranti dicuri atau digandakan sehingga jatuh ketangan -tangan jahil.
- 3) Ijin didasarkan atas apa yang Anda ketahui : Sistem akses yang umum, namun ada kelemahan yang cukup

mencolok. Contohnya adalah password rahasia, kombinasi kunci atau nomor identifikasi pribadi (PIN). Kelemahan yang paling mencolok dari sistem ini adalah karena pengetahuan tentang identifikasi tersebut (misalnya : password rahasia) harus dilindungi. Password harus dipilih secara hati-hati; password harus unik, tidak dapat diterka dan mudah diingat. Password dan kombinasi kunci bisa saja terlewat atau apabila ditulis di suatu tempat, dapat ditemukan dan dicuri oleh orang lain tanpa meninggalkan bukti bahwa pencuri telah mengambilnya.

Banyak Local Area Network (LAN) yang tidak memiliki informasi peka mengandalkan sistem akses jaringan berdasarkan password. Berikut tersaji prinsip pemilihan, penyimpanan, penggunaan dan pembaruan password guna mencapai tingkat keamanan dan efektifitas maksimum:

- Gunakan password dengan panjang paling sedikit enam karakter. Semakin panjang password, semakin lama yang dibutuhkan untuk menerkanya. Semakin lama waktu yang dibutuhkan oleh seseorang untuk masuk ke dalam sistem Anda, semakin kecil kemungkinan mereka akan mencobanya.
- Gunakan password yang mengkombinasi huruf dan angka. Jauh lebih sulit diterka dibandingkan nama atau kata sederhana. Sekalipun Anda hanya menyisipkan satu angka di dalam password berisi delapan karakter yang lazim, namun bagi *hacker* masalahnya menjadi sangat rumit.
- Kebanyakan sistem operasi jaringan dapat mengunci pengguna setelah melakukan beberapa kali upaya memasukkan password yang tidak tepat. Gunakan fasilitas ini apabila Anda sanggup. Hal ini akan menciutkan hati seseorang yang



- berupaya masuk ke dalam sistem Anda dengan menggunakan perangkat lunak penerka password otomatis.
- Ganti password secara teratur. Sampai beberapa teratur tergantung nyaman tidaknya perasaan Anda melakukan hal itu. Ganti password setiap hari apabila ada data yang sangat peka dan cenderung mengundang para *hacker* berbakat melakukan akses tidak sah (contoh data semacam ini adalah record nilai mahasiswa). Anda dapat mengganti password dengan interval waktu yang lebih longgar apabila data kurang begitu peka atau terlalu berharga dimata orang-orang yang tidak berhak melakukan akses (misalnya record bisnis yang tidak melibatkan rahasia dagang).
- Pengguna dengan hak akses luas serta memiliki kekuasaan yang besar untuk mengubah sistem (misalnya, penyelia jaringan) harus lebih sering lagi mengganti password mereka. Sedang mereka yang memiliki hak akses lebih sedikit dapat mengganti password dengan interval waktu yang lebih longgar.
- Meskipun kelihatannya sangat ekstrim, Anda mungkin perlu memperbarui password untuk setiap orang dalam sistem Anda apabila seorang karyawan yang sangat ahli dalam bidang komputasi - terutama kalau sifatnya pemarah atau Jahat - meninggalkan perusahaan.
- Apabila Anda merasa bahwa Anda dapat melakukannya, pilih password untuk pengguna Anda dan bukan memungkinkan mereka memilihnya sendiri. Mereka pasti, tidak senang, tetapi pengguna yang sembrono cenderung memilih password yang mudah diterka (nomor telepon, nama marga, nama pacar, nama anak, tanggal lahir).
- Jangan sekali-kali menyimpan password Anda dalam bentuk tertulis atau di manapun juga pada jaringan kecuali sudah di-*encrypt* oleh sistem. Jangan beritahu password Anda ke orang lain atau apabila hal itu harus dilakukan, ganti segera setelah Anda melakukannya, jangan sampai terdengar oleh telinga dan terlihat oleh mata.

Berikut adalah contoh hakakses direktori dan file dari pengguna NovellNetware (Currid, 1993)

HAK	Fungsi
<i>Read</i> (Membaca)	Mengizinkan user untuk membaca atau melihat isi file
<i>Write</i> (Menulis)	Mengizinkan user untuk memodifikasi file yang ada
<i>Open</i> (Membuka)	Mengizinkan user untuk dapat membuka file yang ada
<i>Create</i> (Membuat)	Mengizinkan user untuk membuat file/subdirektori baru
<i>Delete</i> (Menghapus)	Mengizinkan user untuk dapat menghapus file dan direktori
<i>Search</i>	Mengizinkan user untuk menampilkan daftar file yang ada dalam satu direktori
<i>Modify</i> (Memodifikasi)	Mengizinkan user untuk dapat mengubah nama file dan atribut-atribut file dalam satu direktori
Parental	Mengizinkan user untuk membuat, mengganti nama, atau menghapus subdirektori didalam direktori (user harus juga mempunyai hak <i>create</i> , <i>modify</i> dan <i>delete</i> )

## b. Firewall

Sasaran keamanan firewall adalah memungkinkan akses publik ke bagian-bagian tertentu dari sistem Anda dan mencegah akses ke bagian-bagian lain. Perangkat lunak untuk tugas ini adalah Firewall. Firewall adalah sistem keamanan yang secara selektif menolak seluruh akses ke bagian-bagian yang telah ditetapkan dari jaringan Anda, berdasarkan cara pengaksesan jaringan. Misalnya, apabila seseorang hendak mengakses *workstation* dengan menggunakan modem, maka yang terlihat hanyalah file dan direktori yang telah ditetapkan. Dimata pengguna jarak jauh, fasilitas jaringan lain tidak ada. Namun pengguna lokal di *workstation* yang sama mungkin dapat mengakses layanan dalam jumlah yang lebih banyak (seperti printer atau file server tambahan)

## 7. MENGGUNAKAN ANTRIAN DAN PRINT SERVER

Keuntungan utama yang diperoleh dari local area network (LAN) ialah kemampuan untuk memakai peralatan mahal secara bersama, seperti Printer berwarna, Printer laser dan ploter. Bila komputer *stand-alone* mencetak pada printer yang terpasang padanya, maka kerja cetakan diberikan langsung dari komputer ke peralatan pencetak. Dalam lingkungan jaringan, permintaan mencetak masih tetap dapat dikirimkan ke printer yang terpasang lokal (jika ada), atau dapat memberikannya ke printer jaringan. Kerja cetakan yang dikirim ke printer jaringan harus dikoordinasikan dengan permintaan untuk mencetak yang berasal dari beberapa *workstation* lain. Ini adalah fungsi dari antrian dan *print server*.

Ketika user menginisialisasi kerja cetakan pada LAN, maka kerja tersebut tidak dikirim langsung ke printer jaringan, melainkan antrian cetakan pada file server. Disini kerja cetakan disimpan sampai printer siap untuk mencetak permintaan tersebut. Print server memantau kesipan printer tersebut dan mengirimkan

permintaan untuk mencetak ke printer dengan cara pesan. Manajemen printer berkisar pada penanganan antrian cetak (*print queue*) yaitu *utility* yang menyimpan permintaan kerja pencetakan dan mengarahkannya ke print server secara berurutan. Proses antrian ini dan pengiriman transmisi printer kadang-kadang disebut sebagai pemetaan printer.

Selain itu, Vendor-vendor *third-party* memasarkan produk-produk tambahan yang memperluas pilihan-pilihan printer dengan menambah print server jaringan yang tidak langsung dikelola oleh pihak server. Produk-produk ini memungkinkan untuk menset lokasi pencetak tambahan yang secara fisik tidak terpasang pada file server.

Printer modern sekarang ini dapat digunakan langsung pada jaringan (*network-aware*). Artinya printer ini sudah dilengkapi dengan *network interface card*-nya sendiri dan dapat langsung dipasang ke kabel Jaringan.

Manager jaringan dapat mengotomatisasi jadwal pencetakan dengan memungkinkan kerja pencetakan disimpan dan di kirim ke printer setelah beberapa waktu tertentu, bilamana tidak terdapat lalu-lintas jaringan lainnya pada sistem yang dapat memperlambat proses pencetakan.

Kenyataannya, pemakaian bersama sebuah printer diantara beberapa user jaringan menyebabkan derajat kerumitan menjadi lebih tinggi daripada dalam keadaan *stand-alone*. Tetapi dengan fleksibilitas dan alat-alat pencetakan yang ada sekarang ini, menjadikan kerumitan ini menjadi keuntungan bagi user.

## 8. KESIMPULAN

Dari pembahasan diatas dapat ditarik kesimpulan bahwa keberhasilan jaringan komputer sangat ditentukan oleh siapa yang mengelolanya. Sistem jaringan komputer yang dibuat bukanlah mutlak dapat membuat bisnis lebih sukses, hanya saja dapat mengoptimalkan sistem yang ada, komputer tidak dapat

mengubah sistem yang buruk menjadi sistem yang baik.

Dengan manajemen jaringan komputer yang tepat, yang didukung dengan seorang Administrator yang bertanggung jawab atas kinerja sistem jaringan komputer, merupakan komponen paling penting dalam sistem jaringan tersebut, sangat menentukan dalam keberlanjutan suatu jaringan komputer.

## DAFTAR PUSTAKA

1. Currid, Cherryl C. & Gillet, Craig A., *Menguasai Novell Netware*, Elex Media Komputindo, 1993
2. Lukas Tanutama dan Hosea Tanutama, *Mengenal Local Area Network (LAN)*, Elex Media Komputindo, 1991
3. Robert M. Thomas, *Pengantar Local Area Network (LAN)*, Elex Media Komputindo, 1996
4. Stallings, W. *Local Network*, Macmillan Publishing Company, 1985.
5. Tanenbaum, AS, *Computer Networks*, Prentise Hall, 1996